TECHNICAL SECURITY ADVISORY

from the
Architecture, Standards & Information Security Office
U. S. Department of Energy

99-02

SUBJECT: TELECOMMUTING

March 1999

What is telecommuting? Telecommuting describes a specific computing environment which pertains to the use of automated information resources over a distance to accomplish work. The use of modems for dial-out/dial-in has always held some risk. Now that telecommuting has become so popular it has increased the risks to our systems.

Dial-in access by modems creates a potential backdoor and could possibly negate all protection provided by a firewall or similar perimeter protection devices. It doesn't make sense to install a firewall and not control remote access. It only takes one captured password or uncontrolled line to enable a backdoor around the firewall. Consideration should be given to what the consequences would be if a hacker gained access to a system at the same level as an employee. What systems and what information could be compromised?

Among the security tools available for system administrators are those that can enhance system security, provide audit capability, and detect intruders. Some of these security tools can be found at http://cio.doe.gov/ucsp/security1.htm. Consideration should also be given to using a security tool to locate unauthorized modems.

One of the best ways to prevent having passwords "stolen" is to use one-time passwords. These are usually generated at the beginning of a session by a smart card or other mechanism, and are good only for that communication session.

Site procedures should be in place and address:

- Requirements for obtaining authorization to use a modem.
- Consequences of using unauthorized modems.
- User responsibilities, including what action to take if a security breach is detected.

Remote access is not a trend; it is here to stay. Be prepared by having policies and procedures in place, conducting regular reviews, and by using security tools on a regular basis.

For questions or assistance contact Philip Sibert on (301) 903-4880.

David K. Berkau

David K. Berkau, Director
Office of Architecture, Standards and Information Security
Office of the Chief Information Officer